Public Key Cryptosystem and Binary Edwards Curves on the Ring $\mathbb{F}_{2^n}[e], e^2 = e$

Moha ben taleb Elhamam
FSDM
Sidi Mohamed Ben Abdellah University
Fez, Morocco.
mohaelhomam@gmail.com
Abdelhakim Chillali
FP, LSI
Sidi Mohamed Ben Abdellah University
Taza, Morocco.
abdelhakim.chillali@usmba.ac.ma
Lhoussain El Fadil
FSDM
Sidi Mohamed Ben Abdellah University
Fez, Morocco.
lhouelfadil2@gmail.com

Journal of Digital Information Management

ABSTRACT: *Let $\mathbb{F}_{2^n}[e]$ be a finite ring of characteristic 2, where $e^2 = e$ and n is a positive integer. Let (a, d) 2 $(\mathbb{F}_{2^n}[e])^2$, such that a and $d + a^2 + a$ are invertible in $\mathbb{F}_{2^n}[e]$, we study the binary Edwards curve over this ring, denoted by $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ and we give a bijection between this curve and produces two binary Edwards curves defined on the finite field $\mathbb{F}_{2^n}$. Afterthat we study the addition law of binary Edwards curves over the ring $\mathbb{F}_{2^n}[e]$. We end this work with cryptography applications, ElGamal twisted Edwards curve cryptosystem and Cramer-Shoup twisted Edwards curve cryptosystem.*

Subject Categories and Descriptors: [E.3 DATA ENCRYPTION]: Public key cryptosystems [**G.1.8 Partial Differential Equations]** Finite element methods

General Terms: Data Encryption, Cryptographic Systems, Finite Elements

Keywords: Binary Edwards curves, Addition law, Finite Ring, Finite Field, Local Ring, Cryptography, encryption, decryption

Received: 11 August 2021, Revised 30 November 2021, Accepted 14 December 2021

Review Metrics: Review Scale: 0-6; Review Score: 4.36; Inter-reviewer consistency: 72.5%

DOI: 10.6025/jdim/2022/20/1/25-30

1. Introduction

In 2007, Edwards [1] introduced a new normal form of elliptic curves on a field K with a characteristic other than 2. Bernstein et al [2], introduces twisted Edwards curves with an equation:

$$(aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2.$$

For $Z \neq 0$ the homogeneous point $(X : Y : Z)$ represents the affine point $(X/Z; Y/Z)$; and presented explicit formulas for addition and doubling over a finite field, the group operations on Edwards curves were faster than those of most other elliptical curve models known at the time.

In [3], M. Boudabra and A. Nitaj gived us A New Public Key Cryptosystem Based on Edwards Curves. They studied of the twisted Edwards curves on the finite field $Z = pZ$ where $p \geq 5$ is a prime number, and generalize it to the rings $Z = p^rZ$ and $Z = p^rq^sZ$:

In [4], D. J. Bernstein et al introduces a new shape for ordinary elliptical curves on the fields of characteristic 2 and give the first complete addition formulas for the binary elliptic curves.

In this work we study twisted Edwards curves on the ring-

$\mathbb{F}_q[e], e^2 = e$. The motivation for this paper is the search for new groups of points of a binary Edwards curve over a finite ring, where the complexity of the discrete logarithm calculation is good for using in cryptography.

Let $\mathbb{F}_{2^n}$ be a finite field of characteristic 2 and order 2^n where n is a positive integer and $\frac{\mathbb{F}_{2^n}[X]}{\langle X^2 - X\rangle}$ the quotient ring of the polynomial ring $\mathbb{F}_{2^n}[X]$ by the ideal generated by (X^2 - X).

This ring can be identified to the finite ring $\mathbb{F}_{2^n}[e]$ where $e^2 = e$. In this work we study binary Edwards curves on the ring $\mathbb{F}_{2^n}[e], e^2 = e$, we give the relation between binary Edwards curves over a finite field and binary Edwards curves over this ring.

We started this work by studying the arithmetic of the ring $\mathbb{F}_{2^n}[e]$, $e^2 = e$ where we show a useful formulae to compute the product law. By this efficient formulae we characterize the set of invertible elements in the ring $\mathbb{F}_{2^n}[e]$, $e^2 = e$ and we show that the set of non invertible elements is the union of the two distinct ideals $\langle e\rangle$ and $\langle 1 - e\rangle$, which proves that $\mathbb{F}_{2^n}[e]$ is not a local ring, we define the binary Edwards curves $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ over this ring and define two binary Edwards curves: $E_{B,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n})$ and $E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n})$ defined over the finite field $\mathbb{F}_{2^n}$ .In the next of this section, we present the elements of $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ and we give a bijection between the two sets: $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ and $E_{B,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n}) \times E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n})$, where π_0 and π_1 are two surjective morphisms of rings defined by:

$$\begin{array}{rcccl} \pi_0 & : & \mathbb{F}_{2^n}[e] & \to & \mathbb{F}_{2^n} \\ & & x_0 + x_1 e & \to & x_0 \end{array} \quad \text{and}$$

$$\begin{array}{rcccl} \pi_1 & : & \mathbb{F}_{2^n}[e] & \to & \mathbb{F}_{2^n} \\ & & x_0 + x_1 e & \to & x_0 + x_1 \end{array}$$

We study the addition law of binary Edwards curves over the ring $\mathbb{F}_{2^n}[e]$, where $e^2 = e$. In this case, we define the additive law $P + Q$ in $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ by $P+Q = \tilde{\pi}^{-1}(\tilde{\pi}(P)+\tilde{\pi}(Q))$ for all points P and Q in $E_{B,a,d}(\mathbb{F}_{2^n}[e])$.

Other purpose of this paper is the applications of $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ in cryptography, we give ElGamal cryptosystem and Cramer-Shoup cryptosystem on $E_{B,a,d}(\mathbb{F}_{2^n}[e])$.

2. THE RING $\mathbb{F}_{2^n}[e], e^2 = e$

$\mathbb{F}_{2^n}$ be a finite field of characteristic 2 and order 2^n where n is a positive integer. The ring $\mathbb{F}_{2^n}[e], e^2 = e$ can be constructed as an extension of the finite field $\mathbb{F}_{2^n}$ by using the quotient ring of the polynomial ring $\mathbb{F}_{2^n}[X]$ by the polynomial $\mathbb{F}_{2^n}[X]$. An element $X \in \mathbb{F}_{2^n}[e]$ is represented by $X = x_0 + x_1 e$ where $(x_0, x_1) \in (\mathbb{F}_{2^n})^2$.

The arithmetic operations in $\mathbb{F}_{2^n}[e]$ can be decomposed into operations in $\mathbb{F}_{2^n}$ and they are computed as follows:

$$X + Y = (x_0 + y_0) + (x_1 + y_1)e$$

and

$$X.Y = (x_0 y_0) + (x_0 y_1 + x_1 y_0 + x_1 y_1)e,$$

where X and Y are two elements in $\mathbb{F}_{2^n}[e]$ represented by $X = x_0 + x_1 e$ and $Y = y_0 + y_1 e$ with coefficients x_0, x_1, y_0 and y_1 are in the field $\mathbb{F}_{2^n}$. The following results can easily be verified:

- $(\mathbb{F}_{2^n}[e], +, .)$ is a finite unitary commutative ring.
- $\mathbb{F}_{2^n}[e]$ is a vector space over $\mathbb{F}_{2^n}$ of dimension 2 and $\{1, e\}$ is it's basis.
- $X.Y = (x_0 y_0) + ((x_0 + x_1)(y_0 + y_1) - x_0 y_0)e.$
- $X^2 = x_0^2 + x_1^2 e.$
  $X^3 = x_0^3 + ((x_0 + x_1)^3 - x_0^3)e.$

Let $X = x_0 + x_1 e \in \mathbb{F}_{2^n}[e]$, X is invertible if and only if $x_0 \not\equiv 0 \ mod\ 2$ and $x_0 + x_1 \not\equiv 0 \ mod\ 2,$, in this case:

- $X^{-1} = x_0^{-1} + ((x_0 + x_1)^{-1} - x_0^{-1})e.$

X is not invertible if and only if $x_0 \equiv 0 \ mod\ 2$ or $x_0 + x_1 \equiv 0 \ mod\ 2$.

- $\mathbb{F}_{2^n}[e]$ is a non local ring.

For all $X \in \mathbb{F}_{2^n}$, we have:

$X = \pi_0(X) + (\pi_1(X) - \pi_0(X))e, Xe = \pi_1(X)e$ and $X(1-e) = \pi_0(X)(1-e)$:

π_0 and π_1 are two surjective morphisms of rings.

3. Binary Edwards Curves Over the Ring $\mathbb{F}_{2^n}[e], e^2 = e$

Let a *and* d are two elements in the ring $\mathbb{F}_{2^n}[e]$, such that a *and* $d + a_2 + a$ are invertible.

We define a binary Edwards curve over the ring $\mathbb{F}_{2^n}[e]$, as a affine curve , which is given by the equation:

$$a(X + Y) + d(X^2 + Y^2) = XY + XY(X + Y) + X^2 Y^2$$

We denote this curves by: $E_{B,a,d}(\mathbb{F}_{2^n}[e])$.

$E_{B,a,d}(\mathbb{F}_{2^n}[e]) = \{(X,Y) \in (\mathbb{F}_{2^n}[e])^2 \mid a(X+Y)+d(X^2+Y^2) = XY + XY(X+Y) + X^2Y^2\}$

Proposition 1: Let a *and* d are in the ring $\mathbb{F}_{2^n}[e]$ then, $d + a^2 + a$ is invertible if and only if $d_0 \neq a_0^2 + a_0$ and $d_0 + d_1 \neq (a_0+a_1)^2 + a_0 + a_1$ in $\mathbb{F}_{2^n}$:

Proof. We have:

$$\begin{aligned} d + a^2 + a &= d_0 + d_1 e + (a_0 + a_1 e)^2 + a_0 + a_1 e \\ &= d_0 + d_1 e + a_0^2 + a_1^2 e + a_0 + a_1 e \\ &= d_0 + a_0^2 + a_0 + (d_1 + a_1^2 + a_1)e, \end{aligned}$$

so $d + a^2 + a$ is invertible if and only if $d_0 \neq a_0^2 + a_0$ and $d_0 + d_1 \neq a_0^2 + a_0 + a_1^2 + a_1$ in $\mathbb{F}_{2^n}$:

Corrolary 2:
a is invertible if and only if $\pi_0(a) \neq 0$ and $\pi_1(a) \neq 0$ in $\mathbb{F}_{2^n}$:

$d + a^2 + a$ is invertible in $\mathbb{F}_{2^n}[e]$ if and only if $\pi_0(d) = \pi_0(a^2 + a)$ and $\pi_1(d) = \pi_1(a^2 + a)$ in $\mathbb{F}_{2^n}$:

Using corrolary 2, if a and $d + a^2 + a$ are invertible in $\mathbb{F}_{2^n}[e]$, then $E_{B,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n})$ and $E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n})$ are two binary Edwards curves over the finite field $\mathbb{F}_{2^n}$, and we notice:

$$E_{B,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n}) = \{(x,y) \in \mathbb{F}_{2^n}^2 \mid a_0(x+y) + d_0(x^2 + y^2) = xy + xy(x+y) + x^2y^2\},$$
$$E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n}) = \{(x,y) \in \mathbb{F}_{2^n}^2 \mid (a_0+a_1)(x+y) + (d_0+d_1)(x^2+y^2) = xy + xy(x+y) + x^2y^2\}.$$

Theorem 3: Let X, Y in $\mathbb{F}_{2^n}[e]$, then $(X,Y) \in E_{B,a,d}(\mathbb{F}_{2^n}[e])$ if and only if $(\pi_i(X), \pi_i(Y)) \in$, $E_{B,\pi_i(a),\pi_i(d)}(\mathbb{F}_{2^n})$, for $i \in \{0,1\}$.

Proof. We have

$$\begin{aligned} a(X+Y) + d(X^2+Y^2) &= (a_0 + a_1 e)(x_0 + x_1 e + y_0 + y_1 e) + (d_0 + d_1 e)((x_0 + x_1 e)^2 + (y_0 + y_1 e)^2) \\ &= (a_0 + a_1 e)[(x_0 + y_0) + (x_1 + y_1)e] + (d_0 + d_1 e)[(x_0^2 + y_0^2) + (x_1^2 + y_1^2)e] \\ &= a_0(x_0 + y_0) + [(a_0 + a_1)(x_0 + x_1 + y_0 + y_1) - a_0(x_0 + y_0)]e + d_0(x_0^2 + y_0^2) + [(d_0 + d_1)(x_0^2 + x_1^2 + y_0^2 + y_1^2) - d_0(x_0^2 + y_0^2)]e \\ &= a_0(x_0 + y_0) + d_0(x_0^2 + y_0^2) + [(a_0 + a_1)(x_0 + x_1 + y_0 + y_1) - a_0(x_0 + y_0) + (d_0 + d_1)(x_0^2 + x_1^2 + y_0^2 + y_1^2) - d_0(x_0^2 + y_0^2)]e, \end{aligned}$$

$$\begin{aligned} XY + XY(X+Y) + X^2Y^2 &= (x_0 + x_1 e)(y_0 + y_1 e) + (x_0 + x_1 e)(y_0 + y_1 e)(x_0 + x_1 e + y_0 + y_1 e) + (x_0 + x_1 e)^2 (y_0 + y_1 e)^2 \\ &= x_0 y_0 + [(x_0 + x_1)(y_0 + y_1) - x_0 y_0]e + (x_0 y_0 + [(x_0 + x_1)(y_0 + y_1) - x_0 y_0]e)[(x_0 + y_0) + (x_1 + y_1)e] + (x_0^2 + x_1^2 e)(y_0^2 + y_1^2 e) \\ &= x_0 y_0 + [(x_0 + x_1)(y_0 + y_1) - x_0 y_0]e + x_0 y_0 (x_0 + y_0) + [(x_0 + x_1)(y_0 + y_1)(x_0 + y_0 + x_1 + y_1) - x_0 y_0 (x_0 + y_0)]e + x_0^2 y_0^2 + [(x_0^2 + x_1^2)(y_0^2 + y_1^2) - x_0^2 y_0^2]e \\ &= x_0 y_0 + x_0 y_0 (x_0 + y_0) + x_0^2 y_0^2 + [(x_0 + x_1)(y_0 + y_1) - x_0 y_0 + (x_0 + x_1)(y_0 + y_1)(x_0 + y_0 + x_1 + y_1) - x_0 y_0 (x_0 + y_0) + (x_0^2 + x_1^2)(y_0^2 + y_1^2) - x_0^2 y_0^2]e. \end{aligned}$$

Or {1, e} is a basis $\mathbb{F}_{2^n}$ vector space $\mathbb{F}_{2^n}[e]$, then, $a(X+Y) + d(X^2+Y^2) = XY + XY(X+Y) + X^2Y^2$ if and only if

$$a_0(x_0 + y_0) + d_0(x_0^2 + y_0^2) = x_0 y_0 + x_0 y_0 (x_0 + y_0) + x_0^2 y_0^2,$$

and

$$(a_0 + a_1)(x_0 + x_1 + y_0 + y_1) + (d_0 + d_1)(x_0^2 + x_1^2 + y_0^2 + y_1^2) = (x_0 + x_1)(y_0 + y_1) + (x_0 + x_1)(y_0 + y_1)(x_0 + y_0 + x_1 + y_1) + (x_0^2 + x_1^2)(y_0^2 + y_1^2).$$

Corrolary 4: The mappings $\tilde{\pi_0}$ and $\tilde{\pi_1}$ are well defined, where $\tilde{\pi_i}$ for $i \in \{0,1\}$; is given by:

$$\begin{array}{cccc} \tilde{\pi_i} & : & E_{B,a,d}(\mathbb{F}_{2^n}[e]) & \to & E_{B,\pi_i(a),\pi_i(d)}(\mathbb{F}_{2^n}) \\ & & (X,Y) & \mapsto & (\pi_i(X), \pi_i(Y)). \end{array}$$

Proposition 5: The $\tilde{\pi}$ mapping defined by:

$$\begin{array}{cccc} \tilde{\pi} & : & E_{B,a,d}(\mathbb{F}_{2^n}[e]) & \to & E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n}) \times E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n}) \\ & & (X,Y) & \mapsto & ((\pi_0(X), \pi_0(Y)), (\pi_1(X), \pi_1(Y))), \end{array}$$

is a bijection.

Proof. As $\tilde{\pi_0}$ and $\tilde{\pi_1}$ are well defined, then $\tilde{\pi}$ is well defined.

• Let $((x_0, y_0), (x_1, y_1)) \in E_{B,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n}) \times E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n})$, then $(x_0 + (x_1 - x_0)e, y_0 + (y_1 - y_0)e) \in E_{B,a,d}(\mathbb{F}_{2^n}[e])$ and it is clear that

hence $\tilde{\pi}$ is a surjective mapping.

Let (X, Y) and (X', Y') be elements of $E_{B,a,d}(\mathbb{F}_{2^n}[e])$, where $X = x_0 + x_1 e$, $Y = y_0 + y_1 e$, $X' = x'_0 + x'_1 e$ and $Y' = y'_0 + y'_1 e$.

If $\tilde{\pi}(X,Y) = \tilde{\pi}(X',Y')$, then

$$\begin{cases} (x_0, y_0) = (x'_0, y'_0) \\ and \\ (x_0 + x_1, y_0 + y_1) = (x'_0 + x'_1, y'_0 + y'_1), \end{cases}$$

so $x_0 = x'_0$, $y_0 = y'_0$, $x_1 = x'_1$ and $y_1 = y'_1$, so $(X,Y) = (X',Y')$, hence $\tilde{\pi}$ is an injective mapping.

We can easily show that the mapping $\tilde{\pi}^{-1}$ defined by $\tilde{\pi}^{-1}((x_0,y_0),(x_1,y_1)) = (x_0+(x_1-x_0)e, y_0+(y_1-y_0)e)$ is the inverse of $\tilde{\pi}$.

Corrolary 6: $\tilde{\pi}_0$ is a surjective mapping.

Proof. For all $(x,y) \in E_{B,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n})$; we have: $(x,y) = \tilde{\pi}_1(xe, ye)$

Corrolary 7: $\tilde{\pi}_1$ is a surjective mapping.

Proof. For all $(x,y) \in E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n})$; we have: $(x,y) = \tilde{\pi}_1(xe, ye)$:

Corrolary 8: The cardinal of the binary Edwards curve $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ is equal to the cardinal of $E_{B,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n}) \times E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n})$

Corrolary 9: Lets P *and* Q two points in the binary Edwards curve $E_{B,a,d}(\mathbb{F}_{2^n}[e])$, then: $P = Q \Leftrightarrow \tilde{\pi}(P) = \tilde{\pi}(Q) \Leftrightarrow \tilde{\pi}_0(P) = \tilde{\pi}_0(Q)$ and $\tilde{\pi}_1(P) = \tilde{\pi}_1(Q)$

4. Addition Formulas in $E_{B,a,d}(\mathbb{F}_{2^n}[e]), e^2 = e$

In [4] presents an addition law for the binary Edwards curve $E_{B,\pi_i(a),\pi_i(d)}(\mathbb{F}_{2^n})$ and proves that the addition law corresponds to the usual addition law on an elliptic curve in Weierstrass form. One consequence of the proof is that the addition law on $E_{B,\pi_i(a),\pi_i(d)}(\mathbb{F}_{2^n})$ is strongly unified: it can be used with two identical inputs, i.e., to double.

Given (x_1, y_1) and (x_2, y_2) on the binary Edwards curve $E_{B,\pi_i(a),\pi_i(d)}(\mathbb{F}_{2^n})$, compute the sum $(x_1, y_3) = (x_1, y_1) + (x_2, y_2)$ if it is defined:

$$x_3 = \frac{\pi_i(a)(x_1+x_2) + \pi_i(d)(x_1+y_1)(x_2+y_2) + (x_1+x_1^2)(x_2(y_1+y_2+1)+y_1y_2)}{\pi_i(a) + (x_1+x_1^2)(x_2+y_2)}$$

$$y_3 = \frac{\pi_i(a)(y_1+y_2) + \pi_i(d)(x_1+y_1)(x_2+y_2) + (y_1+y_1^2)(y_2(x_1+x_2+1)+x_1x_2)}{\pi_i(a) + (y_1+y_1^2)(x_2+y_2)}$$

If the denominators $\pi_i(a) + (x_1+x_1^2)(x_2+y_2)$ and $\pi_i(a) + (y_1+y_1^2)(x_2+y_2)$ are nonzero then the sum (x_3, y_3) is a point on $E_{B,\pi_i(a),\pi_i(d)}$.

Remark 1: As $\tilde{\pi}$ is a bijection mapping between the two sets $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ and $E_{B,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n}) \times E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n})$, then for all points P *and* Q in $E_{B,a,d}(\mathbb{F}_{2^n}[e])$,, we define the additive law $P+Q$ in $E_{B,a,d}(\mathbb{F}_{2^n}[e])$, by $P+Q = \tilde{\pi}^{-1}(\tilde{\pi}(P)+\tilde{\pi}(Q))$ The following corollaries can be proved immediately:

Corrolary 10: If $E_{B,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n})$ and $E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n})$ two curves complete, then $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ is a curve complete.

Corrolary 11: Lets (X_1, Y_1) *and* (X_2, Y_2) tow point in $E_{B,a,d}(\mathbb{F}_{2^n}[e])$, and let $(x_i, y_i) = \tilde{\pi}_i(X_1,Y_1) + \tilde{\pi}_i(X_2,Y_2)$, where $i \in \{0,1\}$, then $(X_3, Y_3) = (X_1, Y_1) + (X_2, Y_2)$ is given by:

$X_3 = x_0 + (x_1 - x_0)e,$

$Y_3 = y_0 + (y_1 - y_0)e.$

5. Cryptography Applications

In cryptography applications, we have:

$card(E_{B,a,d}(\mathbb{F}_{2^n}[e]))$ is not a prime number, because it egals to $card(E_{B,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n})) \times card(E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n}))$

$E_{B,a,d}(\mathbb{F}_{2^n}[e])$ and $E_{B,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n}) \times E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n})$ have the same discrete logarithm problem.

In cryptanalysis, if the discrete logarithm problem is easy in $E_{B,a,d}(\mathbb{F}_{2^n}[e])$, then we can easily break the discrete logarithm on $E_{B,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n})$ and $E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n})$, and vice versa.

5.1. ElGamal Binary Edwards Curve Cryptosystem

The binary Edwards curve ElGamal Cryptosystem is an adapted cryptosystem for elliptic curve from the original El-Gamal cryptosystem [9]. Also can be considered as extension of Diffie-Hellman key exchange protocol and its purpose is to encrypt and decrypt messages. It is described as follows:

Suppose Ali wants to send a message to Bachir. First, Bachir has to establish his public key. He chooses an elliptic curve $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ over a finite ring $\mathbb{F}_{2^n}[e], e^2 = e$, such that the discrete log problem is hard for $E_{B,a,d}(\mathbb{F}_{2^n}[e])$.

He also chooses a point P on $E_{B,a,d}(\mathbb{F}_{2^n}[e])$. He chooses a secret integer b and computes $B = bP$. The elliptic curve $E_{B,a,d}(\mathbb{F}_{2^n}[e])$, the finite ring $\mathbb{F}_{2^n}[e], e^2 = e$, and the points

P and B are Bachir public key.
To send the message to Bachir, Ali does the following:

1. Download Bachir public key.

2. Expresses her message as a point $M = M_2 \in E_{B,a,d}(\mathbb{F}_{2^n}[e])$

3. Chooses a secret random integer k and computes $M_1 = kP$:

4. Computes $M_1 = M + kB$:

5. Sends M_1, M_2 to Bachir.

Bachir decrypts by calculating $M = M_2 - bM_1$: Since $M_2 - bM_1 = (M + kB) - b(kP) = M + k(bP) - bkP = M$:

5.2. Cramer-Shoup binary Edwards curve cryptosystem

In [10], Cramer and Shoup gived New Public Key Cryptosystem, in this work we apply Cramer-Shoup cryptosystem for $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ consists essentially in mapping the operations customarily carried out in the multiplicative group Z_p to the set of points of a binary Edwards curve $E_{B,a,d}(\mathbb{F}_{2^n}[e])$, endowed with an additive group operation.

Alice and Bob want to communicate securely, for this they start publicly with integer b, a binary Edwards curve $E_{B,a,d}(\mathbb{F}_{2^n}[e])$, a point $P \in E_{B,a,d}(\mathbb{F}_{2^n}[e])$ of prime order n and the cyclic group $G =< P >$. These elements are the initialization parametrs Cramer-Shoup $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ cryptosystem:

Cramer-Shoup $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ cryptosystem Key generation: The procedure to generate a public in $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ is outlined as follows:

- Bob chooses five random integer $(e_1, e_2, f_1, f_2, s, w)$ from $\{0, 1, ..., n-1\}$

- Bob computes $Q = sP$, $E = e_1P + e_1Q$, $K = f_1P + f_1Q$, $T = wP$.

Then, the public key is $\{P, Q, E, K, T\}$ and the private key is $(e_1, e_2, f_1, f_2, s, w)$.

Cramer-Shoup $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ cryptosystem Encryption: The procedure to endrypt a message (m) to Bob under her public key $\{P, Q, E, K, T\}$ is outlined as follows:

- Alice converts the plaintext message m to a point P_m on the twisted Edwards curve $E_{B,a,d}(\mathbb{F}_{2^n}[e])$.

- Alice chooses a random k from $\{0, 1, ..., n-1\}$, then calculates: $V_1 = kP, V_2 = kQ, u = kT + P_m, \alpha = \mathbb{H}(V_1, V_2, u)$, where H is a collision-resistant hash function, $R = kE + k\alpha K$.

- Bob sends the ciphertext (V_1, V_2, u, R) to Alice.

Cramer-Shoup $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ cryptosystem Decryption: To decrypt this message, with Bob secret key $(e_1, e_2, f_1, f_2, s, w)$:

- Bob computes $\alpha = \mathbb{H}(V_1, V_2, u)$ and verifies that $e_1V_1 + e_2V_2 + \alpha(f_1V_1 + f_2V_2) = R$.

If this test fails, further decryption is aborted and the outout is rejected.

- Otherwise, Bob computes $P_m = u - wV_1$:

The decryption stage correctly decrypts any properly-formed ciphertext, since

$$u - wV_1 = kT + P_m - wkP = kwP + P_m - wkP = P_m:$$

Cramer-Shoup binary Edwards curve cryptosystem is directly based on discrete logarithm problem over (G; +) of base P.

This problem requires to find k where Q = kP and points P, Q belong to a set of points G of a binary Edwards curve $E_{B,a,d}(\mathbb{F}_{2^n}[e])$. It is known to be computationally difficult and this can be utilized to accomplish a more elevated level pf security in cryptosystem.

6. Conclusion

In this work, we have proved the bijection between $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ and $E_{B,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n}) \times E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n})$.

In cryptography applications, we deduce that the discrete logarithm problem in $E_{B,a,d}(\mathbb{F}_{2^n}[e])$ and $E_{B,\pi_0(a),\pi_0(d)}(\mathbb{F}_{2^n}) \times E_{B,\pi_1(a),\pi_1(d)}(\mathbb{F}_{2^n})$ have the same discrete logarithm problem.

Furthermore, we give ElGamal cryptosystem and Cramer-Shoup cryptosystem on $E_{B,a,d}(\mathbb{F}_{2^n}[e])$.

References

[1] Harold M. Edwards. (2007). Normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44 (3) 393-423, April.

[2] Bernstein, D. J., Birkner, P., Joye, M., Lange, T., Peters, C. (2008). Twisted Edwards curves. *In:* Progress in Cryptology — AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008. vol. 5023 of *Lecture Notes in Computer Science*, 389-405. Springer Verlag.

[3] Maher Boudabra., Abderrahmane Nitaj. (2019). A New Public Key Cryptosystem Based on Edwards Curves., *Journal of Applied Mathematics and Computing*, Springer, 2019, 10.1007/s12190-019-01257-y. hal-02321013.

[4] Bernstein, D. J., Lange, T., Rezaeian Farashahi, R. (2008). Binary Edwards Curves. *In:* Oswald E., Rohatgi P. (eds) Cryptographic Hardware and Embedded Systems - CHES 2008. Lecture Notes in Computer Science, vol 5154. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978- 3- 540-85053-3-16.

[5] Ben Taleb, E.M., Chillali, A., El Fadil, L. (2020).Twisted Hessian curves over the Ring *Fq*[*e*]; $e^2 = e$. Bol. Soc. Paran, in press, doi:10.52699/bspm.15867, (2020).

[6] Boulbot, A., Chillali, A., Mouhib, A. (2020). Elliptic Curves Over the Ring R, *Bol. Soc. Paran*. (2020), 38 (3) 193—201.

[7] Boulbot, A., Chillali, A., Mouhib, A. ELLIPTIC CURVES OVER THE RING $F_q[e]$; $e^3 = e^2$, *Gulf Journal of Mathematics,* 4 (4) 123–129.

[8] Huseyin Hisil., Kenneth Koon-Ho Wong., Gary Carter., and Ed Dawson. (2008). Twisted Edwards Curves Revisited J. Pieprzyk (Ed.) *In:* - ASIACRYPT 2008, LNCS 5350, p. 326–343.

[9] ElGamal, Taher. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *In:* Proceedings of CRYPTO 84 on Advances in cryptology, 10-18. Springer-Verlag New York, Inc,1985.

[10] Cramer, Ronald., Shoup, Victor. (1998). A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. Advances in Cryptology - CRYPTO ’98, Springer Berlin Heidelberg, 13-25.